UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

UNITED STATES,	:	
	:	
v.	:	
	:	**Criminal No. 09-0466(BMC)**
JOAQUÍN GUZMÁN LOERA,	:	**Trial Date: 9/5/18**
	:	
Defendant.	:	**UNDER SEAL**[1]

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (DUTCH SERVERS)

Defendant Joaquín Guzmán Loera ("Guzmán"), by and through undersigned counsel, respectfully moves this Court to suppress evidence seized by the government without a warrant from certain communications servers located in the Netherlands (the "Dutch Servers"). In support of this Motion Mr. Guzmán states as follows:

BACKGROUND

This matter is before the Court on a fourth superseding indictment filed on May 11, 2016, which charges Mr. Guzmán and codefendant Ismael Zambada Garcia with a laundry list of offenses, including operating a continuing criminal enterprise (Count 1); participating in a wide-ranging narcotic trafficking conspiracy (Counts 2, 3 and 4); eleven counts of specific acts of distribution of cocaine (Counts 5 through 15); use of a firearm during a drug trafficking crime (Count 16); and conspiracy to launder narcotics proceeds (Count 17).

The government has provided extensive discovery, in effect a document dump without any index, including "more than 320,000 pages of documents, and thousands of intercepted and recorded audio and electronic communications and dozens of videos." Doc. # 229 at 3. On July 3, 2018, the government produced approximately 82G gygabytes of material,

[1] This Motion is filed under seal to comply with the Court's Protective Order.

including over 117,000 sound files and other documents. On July 5, 2018, the government produced approximately 3,500 pages of §3500 material, including unredacted versions of the MLAT requests related to the "Dutch Server." During the continuing review of discovery, the defense became aware of evidence seized by the government without a warrant. Mr. Guzmán now moves to suppress that warrantless seizure of evidence and any other evidence derived from it.

FACTS

In or around 2009, the government began investigating a Colombian drug trafficking organization headed by Jorge Cifuentes-Villa ("Jorge"), which allegedly supplied Mr. Guzmán with cocaine. Jorge's sister, Dolly Cifuentes ("Dolly"), who was in charge of the Cifuentes finances, arranged to create a private communications network for the family. Two confidential sources, CS1 and CS2, assisted Dolly in creating the network. *See generally* Exh. 1; Bates 12135A ¶ 11 - 12.[2]

Through his contacts with the Cifuentes family, CS2 allegedly met Mr. Guzmán in early 2009. According to S.A. Grey, Mr. Guzmán asked CS2 to build him an encrypted communications network similar to the Cifuentes network so that he could communicate with his associates without the risk of government interception. CS2 did so and the network, once based in Canada and then moved to the Netherlands in early April of 2011, went live sometime in late 2009. *Id.* ¶ 13 - 14. CS2 "became a paid confidential source for the FBI in approximately February 2011." *Id.* n.1.

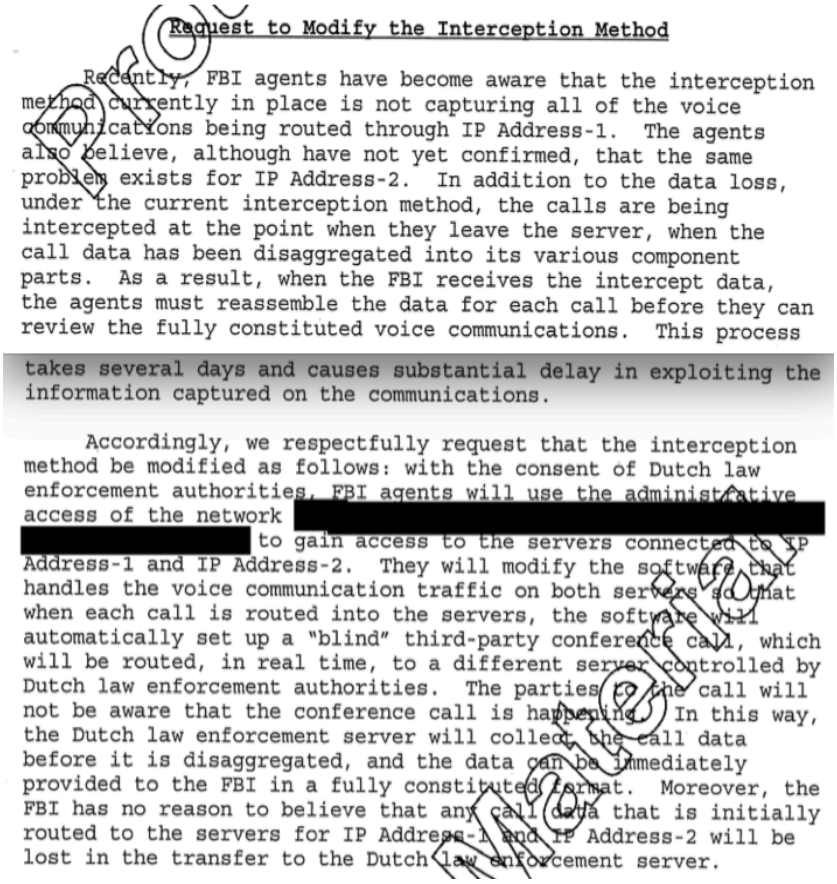
According to the government, the FBI had discovered that certain IP addresses allegedly corresponded to a communications network used by Mr. Guzmán and his associates.

[2] The MLAT requests produced by the government in discovery are heavily redacted. On July 5, 2018, the government produced unredacted copies of the MLAT request as part of its Jencks/§3500 disclosures.

The servers running the network were based in the Netherlands. Beginning approximately on March 30, 2011, and pursuant to the Mutual Legal Assistance Treaty (MLAT) between the United States and the Netherlands, the government requested Dutch authorities to conduct electronic surveillance of IP addresses 95.211.10.71 and 95.211.10.70. Exh. 2; Bates # 11303 – 11306. The government also requested that the information obtained be provided to United States law enforcement authorities on an ongoing basis. *Id.*

On April 4, 2011, the government submitted another MLAT request asking Dutch authorities to conduct electronic surveillance of IP address 83.149.125.226 and that the information obtained be provided to United States law enforcement authorities on an ongoing basis. Exh. 3; Bates # 11311 – 11314. On April 13, 2011, the government submitted another MLAT request asking Dutch authorities to conduct electronic surveillance of IP address 83.149.125.227 and that the information obtained be provided to United States law enforcement authorities on an ongoing basis. Exh. 4; Bates # 11315 – 11319. The government made additional MLAT requests for continued surveillance of the servers using those IP addresses on April 27, 2011, May 4, 2011, May 24, 2011 and June 17, 2011.

On July 18, 2011, the government made another MLAT request asking Dutch authorities to extend the intercept authorization for those three IP addresses. The government also requested to modify the interception method:



Request to Modify the Interception Method

Recently, FBI agents have become aware that the interception method currently in place is not capturing all of the voice communications being routed through IP Address-1. The agents also believe, although have not yet confirmed, that the same problem exists for IP Address-2. In addition to the data loss, under the current interception method, the calls are being intercepted at the point when they leave the server, when the call data has been disaggregated into its various component parts. As a result, when the FBI receives the intercept data, the agents must reassemble the data for each call before they can review the fully constituted voice communications. This process takes several days and causes substantial delay in exploiting the information captured on the communications.

Accordingly, we respectfully request that the interception method be modified as follows: with the consent of Dutch law enforcement authorities, FBI agents will use the administrative access of the network [redacted] to gain access to the servers connected to IP Address-1 and IP Address-2. They will modify the software that handles the voice communication traffic on both servers so that when each call is routed into the servers, the software will automatically set up a "blind" third-party conference call, which will be routed, in real time, to a different server controlled by Dutch law enforcement authorities. The parties to the call will not be aware that the conference call is happening. In this way, the Dutch law enforcement server will collect the call data before it is disaggregated, and the data can be immediately provided to the FBI in a fully constituted format. Moreover, the FBI has no reason to believe that any call data that is initially routed to the servers for IP Address-1 and IP Address-2 will be lost in the transfer to the Dutch law enforcement server.

Exh. 5; Bates 11328 – 11331. The government made additional MLAT requests for continued surveillance of the servers using those IP addresses on August 18, 2011 and September 12, 2011.

Also, on September 12, 2011, the government requested that the "Dutch obtain and execute a search warrant on the computer servers associated with IP Address-1 and IP Address-2, so that the stored communications may be accessed and reviewed by the FBI." Exh.6; Bates # 11341 – 11343. On October 12, 2011, Dutch law enforcement authorities executed the search warrants on the computer servers associated with the IP addresses and provided the government with "imaged copies of those servers. The imaged copies contained, among other things, copies of all the voice communications that were stored on the servers." Exh. 7; Bates # 11349 – 11351. The government made additional MLAT requests for continued surveillance of the servers using those IP addresses on October 12, 2011, October 21,

2011, and November 7, 2011.

On November 8, 2011, the government asked that the Dutch authorities execute periodic search warrants on the servers associated with the IP Addresses and provide the content from the intercepts or search warrants to the FBI on a regular basis. Exh. 8; Bates # 11358 – 11360. On November 10, 2011, the government asked that Dutch authorities allow the FBI to lease server space from the same hosting company in the Netherlands; to configure the servers; and to transfer the stored communications related to the IP addresses to new servers in the Netherlands. The new servers would be controlled by the FBI. Exh. 9; Bates #11361-11364..

On November 21, 2011, the government presented another MLAT request asking Dutch authorities to allow the FBI to create a Backup Server that would continuously receive and store all data stored on the servers associated with the IP addresses and that that Dutch authorities periodically access the data stored on the backup server and share that data with the FBI on a regular basis. Exh. 10; Bates #11365 – 11367.

On December 1, 2011, the government requested that Dutch authorities "tap/collect" data for a new IP address (95.211.15.234. Exh. 11; Bates #11371 – 11372. The government made additional MLAT requests for continued surveillance of the servers using those IP addresses on December 5, 2011.

On January 15, 2012, the government requested that Dutch authorities allow the FBI to rent two additional servers; configure all servers to automatically and continuously transfer the data on the servers to a Backup Server so that the data can be intercepted and collected. Dutch authorities approved this request on January 24, 2012. Exh. 12; Bates # 11376 – 11379.

On February 3, 2012, the government requested that Dutch authorities conduct

electronic surveillance for the Backup Servers. Dutch authorities approved that request on April 11, 2012. The government thereafter sent multiple MLAT requests on May 2, 2012, May 24, 2012, June 26, 2012, July 23, 2012 and August 21, 2012 requesting an extension of surveillance. On October 12, 2012, the government requested that Dutch authorities execute a search warrant to obtain mirror images of the computer servers supporting the Guzmán network so that the stored communications contained in the servers could be accessed and reviewed by United States law enforcement. Exh. 13; Bates # 92999 – 93002. On October 23, 2012, the government submitted another MLAT request specifying the IP addresses covered by the prior requests: 83.149.125.226; 83.149.125.227; 95.211.10.70; 95.211.120.190; 95.211.15.231; 95.211.111.4. Exh. 14; Bates # 92998.

Upon information and belief, Dutch authorities searched and seized multiple voice and text conversations as well as other information pertaining to Mr. Guzmán.

ARGUMENT

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. Const. amend. iv. The "basic purpose of this Amendment," the Supreme Court has recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter v. United States*, 2018 WL 3073916 (June 22, 2018) (citations omitted). The Constitution protects two distinct types of expectations, one involving "searches," the other "seizures." A "search" occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. *See Illinois v. Andreas*, 463 U.S. 765 (1983); *Smith v. Maryland*, 442 U.S. 735, 739-741 (1979). A "seizure" of property occurs when there is some meaningful interference with an individual's

possessory interests in that property, *see, e.g., United States v. Place*, 462 U.S. 696 (1983).

The Supreme Court has held that "the people" described by the text of the Fourth Amendment are persons who are part of the national community or who have otherwise developed sufficient connection with this country to be considered part of that community. However, the Fourth Amendment does not protect non-resident aliens on foreign soil from unreasonable searches and seizures by United States officials. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 265, 271 (1990) (finding that Mexican citizen without a "substantial connection" to the United States was not protected by the Fourth Amendment against an unreasonable search and seizure of his Mexican residence by U.S. officials). [Unless the investigating foreign government authorities (1) acted on behalf and under instruction of the US government and (2) there was a misconduct on the part of the of the foreign official in the process of the search and seizure, enough to "shock the judicial conscience" or in a situation which restrictions of the Fourth Amendment were clearly being side-stepped.

Dutch Authorities Acted as Agents of the Government

The foreign search must be the result of American law-enforcement action. If a foreign government conducts the search alone, the Fourth Amendment does not serve to exclude the fruits of even a clearly-unlawful search or seizure. *See United States v. Benedict*, 647 F.2d 928 (9th Cir. 1981) (Fourth Amendment is not applicable to search initiated by the Thai police under Thai law); *United States v. Janis*, 428 U.S. 433, 455 n.1 (1976) (exclusion of illegally-obtained evidence not required where foreign government committed the offending act). But on the other hand, if United States law enforcement officers participate in a foreign search, or if the search is the result of its coordination or an agency relationship between the United States agents and their foreign counterparts, the Fourth Amendment protections may be triggered. *See*

United States v. Maturo, 982 F.2d 57 (2d Cir. 1992); *United States v. Mitro*, 880 F.2d 1480, 1482-84 (1st Cir. 1989).

Fourth Amendment constitutional requirements may attach where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials, *see United States v. Busic,* 592 F.2d 13, 23 n.7 (2d Cir.1978); or where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials. *See United States v. Bagaric,* 706 F.2d 42, 69 (2d Cir.) *cert. denied,* 464 U.S. 840 (1983).

Here, Dutch authorities acted at the behest of, and as agents for, United States law enforcement. Dutch authorities were not conducting their own independent investigation of Mr. Guzmán's communications networks. In fact, the Dutch investigation began only after the government made its initial MLAT request on March 30, 2011, received by the Dutch authorities on April 5, 2011. The application for interception was submitted by the Dutch Public Prosecutor the day after on April 6, 2011, the order was issued the same day by an examining magistrate at the Rotterdam Court. *See, e.g.,* Exh. 15; Bates # 0323007-323009 (excerpt of translated Dutch court orders). Additionally, the government has revealed that it became aware of the Dutch Servers through CS2, a paid informant of the US government, whose information was certainly not available to Dutch authorities prior to the initial MLAT request. Agent Van Dyk states that "at the request of the FBI, and based on the information provided by CS-2, Dutch Law enforcement authorities intercepted the communications passing through these servers…and have shared that information with the FBI. Exh. 16 Bates # 12223A. Finally, there is no evidence that Dutch authorities were investigating or prosecuting Mr. Guzmán prior to the first MLAT request made on March 30, 2011 and received by the Dutch authorities on April 5, 2011.

Nevertheless, at the request of the United States government, Dutch authorities conducted electronic surveillance of the subject servers; executed searches and seizures on those servers and provided the resulting evidence to the government. Exh. 14; Bates # 92998-93119 While it is not sufficient to merely argue that Dutch authorities undertook its investigation pursuant to an American MLAT request, *United States v. Getto*, 729 F.3d 221, 230 (2d Cir. 2013), Dutch authorities in this case allowed the FBI itself to "use the administrative access of the network … to gain access to the servers connected to" the IP addresses and to "modify the software so that when each call is routed into the servers, the software will automatically set up a 'blind' third-party conference call, which will be routed" in real time to a server controlled by Dutch authorities. This modification allowed Dutch authorities to collect all data and pass it on to the FBI. Exh. 5; Bates #11328-11331 Dutch authorities also allowed the FBI to establish their own Backup Server on the Dutch system so that the Dutch authorities could "automatically and continuously transfer the data stored on these servers to the Backup Server where they could be intercepted, collected, and shared with the FBI." Exh. 10; Bates # 11367; Exh. 14; Bates # 93004-93005, # 93009-93010. Therefore, FBI controlled and directed the investigation.

The Fourth Amendment Applies Because
Mr. Guzmán Had Substantial Contacts with the United States

The government may argue that because Mr. Guzmán is a Mexican citizen and the evidence was searched and seized in the Netherlands he does not merit Fourth Amendment protections. However, the government itself has claimed that Mr. Guzmán "and other leaders of the Sinaloa Cartel directed a large-scale narcotics transportation network involving the use of land, air and sea transportation assets, shipping multi-ton quantities of cocaine from South America, through Central America and Mexico and finally into the United States. In addition, the Sinaloa Cartel manufactured and imported multi-ton quantities of heroin, methamphetamine

and marijuana into the United States. The vast majority of drugs trafficked by the Sinaloa Cartel were imported into the United States, where the drugs were consumed." Doc. 14 at 3. The government also alleges that the "Sinaloa Cartel's drug sales in the United States generated billions of dollars in profit. The drug proceeds were then laundered back to Mexico; often the drug money was physically transported from the United States to Mexico in vehicles containing hidden compartments …." *Id.* The government further alleges that "the Mexicans established distribution networks across the United States." Doc. 17 at 6. According to the government, Mr. Guzman "oversees a vast cocaine transportation infrastructure in South and Central America and within Mexico that brings cocaine to Mexico's northern border with the United States. He also maintains an equally formidable transportation infrastructure, which includes the use of tunnels, to smuggle cocaine, heroin, methamphetamine and marijuana over the Mexican-American border to the United States. Guzman uses drug distribution networks throughout the United States, including within the Eastern District of New York, to sell the drugs and obtain multi-billions in cash profits. He also oversees a vast money laundering apparatus which returns the illicit profits to Guzman and his Colombian partners." *Id.* at 17.

Here, the government itself alleges that Mr. Guzmán has substantial and voluntary connections to the United States. Those connections should afford him Fourth Amendment protections. *See Verdugo-Urquidez*, 494 U.S. at 271 (finding that Mexican citizen without a "substantial connection" to the United States was not protected by the Fourth Amendment against an unreasonable search and seizure of his Mexican residence by U.S. officials

Upon information and belief, the government obtained additional evidence derived from the evidence seized from the Dutch Servers. All evidence seized as a result of illegal police activity must be suppressed as the "fruit of the poisonous tree." *Wong Sun v. United*

States, 371 U.S. 471, 488 (1963).

CONCLUSION

WHEREFORE, for the foregoing reasons, and any other that may become apparent to the Court, Mr. Guzmán respectfully requests that this motion be **GRANTED**.

Dated: Washington, DC
July 9, 2018

Respectfully submitted,

BALAREZO LAW

By: _____

A. Eduardo Balarezo, Esq.
EDNY Bar # AB7088
400 Seventh Street, NW
Suite 306
Washington, DC 20004
Tel: (202) 639-0999
Fax: (202) 639-0899
E-mail: aeb@balarezolaw.com

Counsel for Defendant Joaquín Guzmán Loera

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 9th day of July 2018, I caused a true and correct copy of the foregoing Defendant's Motion to Suppress Evidence (Dutch Servers) to be delivered via Electronic Case Filing to the Parties in this case

A. Eduardo Balarezo, Esq.